AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

KEEPSAFE ACCOUNT ASSOCIATED WITH E-MAIL ADDRESS nathanallen88@gmail.com

Case No. 2:21-sw 169

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Attachment A-1

located in the Northern District of California, there is now concealed *(identify theperson or describe the property to be seized)*:

Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251(a)	Sexual exploitation of children for purpose producing visual depiction
18 U.S.C. § 2252(a)(2)	Receipt of a visual depiction of a minor engaged in sexuallyexplicit conduct
18 U.S.C. § 2252(a)(4)(B)	Possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Reviewed by AUSA/SAUSA:

E. Rebecca Gantt, Assistant United States Attorney
Printed name and title

John W. Shields, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Judge's signature

Date: September 23, 2021

Lawrence R. Leonard, U.S. Magistrate Judge
Printed name and title

City and state: Norfolk, VA

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

IN THE MATTER OF THE SEARCH OF:

KEEPSAFE ACCOUNT ASSOCIATED WITH E-MAIL ADDRESS nathanallen88@gmail.com

AND

THE GOOGLE ACCOUNT OF nathanallen88@gmail.com

UNDER SEAL

Case No. 2:21sw 169

Case No. 2:21sw 168

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, John W. Shields, being duly sworn, hereby depose and state:

1. I am a Special Agent (SA) with Homeland Security Investigations (HSI) assigned to Norfolk, Virginia. I have been an Agent with HSI since April 2016. I am currently assigned to the National Security and Child Exploitation Group, which conducts a wide variety of investigations of crimes including crimes where computers and the internet are used in the sexual exploitation of children, including (but not limited to) violations involving producing or trafficking in child pornography. In addition to working on federal investigations, I have worked on child molestation/child sex abuse cases while working for the Lincoln County Sheriff's Office and the Reardan Police Department. In connection with my work in both local and federal law enforcement, I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children to include training programs, participation in the execution of search warrants involving child pornography, and participation in warrants involving seizures of computers and other digital storage media. In addition, I have conducted numerous drug smuggling investigations resulting in the seizure of contraband and the arrest of numerous suspects. The statements contained in this Affidavit are based on my experience and background as a special agent and on information provided by other law enforcement agents.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is submitted in support of an application for a warrant under Rule 41 of the Federal Rules of Criminal Procedure, as well as Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to search and seize the contents of the Keepsafe Software, Inc. ("Keepsafe") account associated with email address "nathanallen88@gmail.com" (the SUBJECT KEEPSAFE ACCOUNT), and the Google LLC ("Google") account associated

with email address "nathanallen88@gmail.com" (the SUBJECT GOOGLE ACCOUNT), (collectively, the SUBJECT ACCOUNTS), described in more detail in Attachments A-1 and A-2 hereto.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. I have set forth only those facts that I believe are necessary to establish probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(2) & (4)(B), which, in relevant part, prohibit the production, receipt, and knowing possession of or access with the intent to view one or more matters containing any visual depictions of and involving the use of a minor engaging in sexually explicit conduct that have traveled in interstate or foreign commerce or were produced using material so transported or shipped are present in the information associated with the SUBJECT ACCOUNTS. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

PERTINENT CRIMINAL STATUTES

5. 18 U.S.C. § 2251(a) prohibits, in relevant part, a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce.

6. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and such visual depiction is of such conduct.

7. 18 U.S.C. § 2252(a)(4)(B) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer.

OTHER LEGAL AUTHORITY

8. The legal authority for this search warrant application regarding the SUBJECT ACCOUNTS is derived from 18 U.S.C. §§ 2701-2713, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides, in relevant part:

a. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and

eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure . . . .

b. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

9. 18 U.S.C. § 2703(b) provides, in relevant part:

a. A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

i. Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . .

b. Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –

i. On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

ii. Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

10. The government may also obtain records relating to electronic communications, such as subscriber identifying information, by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A).

11. 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

12. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated below. *See* 18 U.S.C. §§ 3231, 3237; Fed. R. Crim. P. 18.

DEFINITIONS

13. The following definitions apply to this affidavit and attachments to this affidavit:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Minor" and "sexually explicit conduct" are defined in 18 U.S.C. §§ 2256(1) and (2). A "minor" is defined as "any person under the age of eighteen years." The term "sexually explicit conduct" means actual or simulated:

    1. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral- anal, whether between persons of the same or opposite sex;
    2. Bestiality;
    3. Masturbation;
    4. Sadistic or masochistic abuse; or
    5. Lascivious exhibition of the genitals or pubic area of any person.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. 18 U.S.C. § 1030(e)(1).

d. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

e. "Internet Protocol Address" (IP Address), as used herein, refers to refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. A "natting" IP address is a type of IP address that becomes assigned to multiple devices at the same time when those

devices are connected to a common router (normally the term is invoked when multiple individuals are connected to the same cellular towers and cellular data network. All devices connected to the same tower will be assigned the same "natting" IP Address.)

f. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called "bandwidth," that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

g. "Remote Computing Service" as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

h. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

i. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, log-on/log-off times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

j. "Electronic Communications Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

k. "Electronic Communications System" means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

l. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

m. The terms "records," "documents," and "materials" include all information recorded in any form, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

    1. graphic records or representations;
    2. photographs;
    3. pictures;
    4. images, and
    5. aural records or representations.

n. The terms "records," "documents," and "materials" include all of the foregoing, in whatever form and by whatever means, the records, documents, or materials, and their drafts, or their modifications may have been created or stored, including (but not limited to): any electrical, electronic, or magnetic form (including but not limited to any information on an electronic or magnetic storage device such as hard disks).

o. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

p. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

PROBABLE CAUSE TO SEARCH THE SUBJECT ACCOUNTS

14. On or about April 7th, 2021, HSI TFO Hand, while working in an undercover capacity, accessed the Internet and connected to a BitTorrent network using a law enforcement client program that is used to monitor the trafficking of child pornography occurring over P2P networks. TFO Hand is familiar with P2P file-sharing networks and programs, specifically the operation of the BitTorrent network. This particular BitTorrent network, like other P2P file-sharing networks, uses file hashing to uniquely identify files on the network, and users typically locate files with keyword searches. TFO Hand focused the investigation on IP Address 68.10.229.35, because it was associated with a torrent file referencing 6018 files, of which at least one was identified by law enforcement as a file containing child pornography or being part of a series of files that contain child pornography, based on a hash value of a file contained in the torrent file. Using a computer running investigative BitTorrent software, TFO Hand successfully completed the download of thirty-nine files from the torrent file that the device at IP Address 68.10.229.35 was making available, which files appeared to depict child pornography or child erotica. TFO Hand viewed one of the files, of which one is a video file named, "insta.mp4," that is 03:38 in length, and is a compilation video depicting a prepubescent female who is approximately ten-to-twelve years of age, exposing her vagina and anus for the camera and engaging in self-masturbation with various items including a hairbrush.

15. During the downloading of the above file, other incoming data was captured. TFO Hand confirmed the device at IP address 68.10.229.35 was the sole candidate for each download, and as such, each file was downloaded directly from this IP address.

16. Additionally, on or about April 7th, 2021, TFO Hand downloaded another torrent file from the same IP address which referenced 4461 files, of which at least one was identified by law enforcement as a file containing child pornography or being part of a series of files that contain child pornography, based on a hash value of a file contained in the torrent file. On April 7th, 2021, using a computer running investigative BitTorrent software, TFO Hand successfully completed the download of forty-three files and eight partial files from the torrent file that the device at IP Address 68.10.229.35 was making available, which files appeared to depict child pornography or child erotica. TFO Hand was able to view a portion of one of the files, of which was a video file with file name ending in "00039.avi", approximately thirty-three minutes and fifty-two seconds in length, depicts two nude prepubescent females, approximately eight-to-ten years of age. One girl is sitting on the other girl's lap, with both girls exposing their genitalia for the camera and kissing one another.

17. During the downloading of the above file, other incoming data was captured. TFO Hand confirmed the device at IP address 68.10.229.35 was the sole candidate for each download, and as such, each file was downloaded directly from this IP address.

18. TFO Hand determined Cox Communications to be the Internet Service Provider for IP Address 68.10.229.35 during the time frame of the downloads mentioned in the preceding paragraphs. On or about April 12th, 2021, TFO Hand obtained an administrative subpoena for subscriber information to who leased the IP address 68.10.229.35. On or about May 4th, 2021, Cox Communications identified the customer as Nathan ALLEN, 316 Rose Marie Avenue, Virginia Beach, Virginia 23462 (the "Virginia Beach residence"). The records further indicated that the IP address was leased to that subscriber from 01-28-2021 at 05:04:02 (GMT) to 04-21-2021 at 01:45:21 (GMT).

19. On or about April 29th, 2021, TFO Hand, while working in an undercover capacity, accessed the Internet and connected to a BitTorrent network using a law enforcement client program that is used to monitor the trafficking of child pornography occurring over P2P networks. TFO Hand focused the investigation on IP Address 68.10.91.245, because it was associated with a torrent file referencing thirty-eight files, at least one of which was identified by law enforcement as a file containing child pornography or being part of a series of files that contain child pornography, based on a hash value of a file contained in the torrent file. On April 29th, 2021, using a computer running investigative BitTorrent software, TFO Hand successfully completed the partial downloads of eighteen files from the torrent file that the device at IP Address 68.10.91.245 was making available, which files appeared to depict child pornography or child erotica. TFO Hand was able to view a portion of one of the files, which was a video file with file name ending in "576.MPG", approximately eight minutes and two seconds in length, and a compilation video of a prepubescent female approximately eight-to-ten years of age, nude and engaged in vaginal intercourse with an adult male.

20. During the downloading of the above file, other incoming data was captured. TFO Hand confirmed the device at IP address 68.10.91.245 was the sole candidate for each download, and as such, each file was downloaded directly from this IP address.

21. On or about April 30th, 2021, TFO Hand, while working in an undercover capacity, accessed the Internet and connected to a BitTorrent network using a law enforcement client program that is used to monitor the trafficking of child pornography occurring over P2P networks. TFO Hand focused the investigation on IP Address 68.10.91.245, because it was associated with a torrent file referencing 1719 files, at least one of which was identified by law enforcement as a file containing child pornography or being part of a series of files that contain child pornography, based on a hash value of a file contained in the torrent file. On or about April 30th, 2021, using a computer running investigative BitTorrent software, TFO Hand successfully completed the download of 242 files from the torrent file that the device at IP Address 68.10.91.245 was making available, which files appeared to depict child pornography or child erotica. TFO Hand was able to view a portion of one of the files which is an image file named "lsm07-07-084.jpg" that depicts three nude prepubescent females, approximately ten-to-twelve years of age, sitting on a bed together, with their legs spread open and exposing their genitalia for the camera.

22. During the downloading of the above file, other incoming data was captured. TFO Hand confirmed the device at IP address 68.10.91.245 was the sole candidate for each download, and as such, each file was downloaded directly from this IP address.

23. TFO Hand determined Cox Communications to be the Internet Service Provider for IP Address 68.10.91.245 during the time frame of the downloads discussed in the preceding paragraphs. On or about May 10th, 2021, TFO Hand obtained an administrative subpoena for subscriber information to who leased the IP address 68.10.91.245. On or about May 28th, 2021, Cox Communications identified the customer as Nathan ALLEN, with an address of the Virginia Beach residence. The records further indicated that the IP address was leased to that subscriber from 04-28-2021 at 04:50:29 (GMT) to 05-10-2021 at 07:51:38 (GMT).

24. TFO Hand and other agents conducted physical surveillance at the Virginia Beach residence from on or about June 1st, 2021 to on or about July 29th, 2021. During this timeframe, TFO Hand and other law enforcement agents consistently saw a white 2010 Nissan Altima four door sedan parked there. A Department of Motor Vehicles (DMV) check revealed the registered owners to be Nathan ALLEN Jr. and S.S. of the Virginia Beach residence. Additional police records checks also confirmed the Virginia Beach residence to be the residence of ALLEN and S.S. TFO Hand and other law enforcement agents on several occasions observed a male leave the residence in the Altima; his appearance was consistent with ALLEN's DMV photo as well as photos from ALLEN's public Facebook profile.

25. In addition, TFO Hand observed a silver 2008 Toyota Scion parked at the residence. A DMV check revealed the registered owners to be ALLEN and S.S. of the Virginia Beach residence. On several occasions, ALLEN was observed leaving the residence in the Scion, as well as an adult female whose appearance was consistent with the DMV photo of S.S. Based on surveillance and publicly available records, there were no other adult residents. According to the Virginia Beach School District there were approximately eight children known to live at the residence, ranging in grades from kindergarten to 7th grade.

26. During surveillance, TFO Hand on numerous occasions attempted to determine if an open or unsecure Wi-Fi signal was available in the vicinity of the Virginia Beach residence. TFO Hand and other law enforcement agents were unable to locate an open wireless Wi-Fi signal.

27. On or about July 12th, 2021, detectives were conducting surveillance and observed ALLEN leaving the residence in the Nissan Altima wearing what appeared to be a police uniform. TFO Hand and another detective followed ALLEN to the Kings Mill Police Department near Williamsburg, Virginia. They observed ALLEN wearing a full police uniform including a firearm and driving a marked police vehicle. ALLEN was previously employed by the City of Hampton as a police officer from about February 2020 until about February 2021, confirmed through social media posts and records provided by the Virginia Employment Commission.

28. Agents obtained search warrants for ALLEN's person, the Nissan Altima, the Toyota Scion, and the Virginia Beach residence. *See* 2:21-sw-123, 124,[1] 125, 126, & 135 (signed by U.S. Magistrate Judge Robert J. Krask).

29. On August 3rd, 2021 at about 05:18 am, agents executed the federal search warrant for ALLEN's person, and located a Samsung Galaxy Note 20 cellular telephone. An initial search of device that day revealed a video of a minor child laying in bed that was taken that morning prior to the search warrant execution. The camera showed the child's legs and moved to her buttocks that were covered by her underwear. The camera then zoomed in between the girl's legs for an extreme close-up of her genitals and buttocks. Agents were able to identify the video as being filmed in the Virginia Beach residence and the victim in the video as a minor girl born in 2008 that is ALLEN's stepdaughter ("Jane Doe"). A subsequent forensic review of the device revealed several hundred similar images of Jane Doe. Many of these other images were found in the thumbnail cache, indicated they had been viewed but deleted. The forensic examiner determined that the metadata of many of these images appeared to indicate they had been stored in a Keepsafe account, which application the forensic examiner found installed on the Samsung telephone. ALLEN admitted to creating these images in a post-*Miranda* interview and further recounted an incident where he had created a similar image when Jane Doe was sleeping naked because the air conditioning was not working. (This image was not located on the Samsung cellular phone.)

30. An initial review of ALLEN's Samsung cellular phone also revealed at least two child pornography images of minors other than Jane Doe. The later forensic examination of the cellular phone revealed approximately 284 Child Pornography Photos, 9453 Child Erotica/Age Difficult Photos, 156 Child Exploitative Animation/CGI files, 633 Comparison/Victim ID files. Some of these images matched those that law enforcement had previously downloaded from a device at the Virginia Beach residence.

31. At the search warrant execution, agents also located a SanDisk 64GM microSD card in ALLEN's police vest that contained a deleted file depicting ALLEN setting up a camera in front of the toilet in the bathroom that S.S. identified as the children's bathroom. When asked, ALLEN admitted to setting this up and that it had captured images of several of the children who lived in the home.

32. In a post-*Miranda* interview, ALLEN stated he began searching for child exploitative material after an encounter with a 12-year-old prostitute while ALLEN was a Hampton Police Officer. ALLEN explained he initially began to look for the material to see how easy it was to find because he wanted it stopped. ALLEN stated he primarily used Bing searches to find the material. ALLEN also admitted to using torrent software. ALLEN further admitted to

---

[1] The initial search warrant for ALLEN's person, 2:21-sw-124, which authorized a search in the daytime only, was returned unexecuted because agents later obtained a search warrant for his person authorizing a search at any time of day or night, 2:21-sw-135.

using his cellphone to download and view child exploitative material. ALLEN admitted to using BitTorrent during the timeframe of TFO Hand's downloads. For instance, ALLEN admitted to using BitTorrent to download "no nude" series images, which was one of the many series that were downloaded by TFO Hand. ALLEN admitted to increased BitTorrent activity after he left Hampton PD, during the March to May timeframe. ALLEN admitted to taking videos of Jane Doe and then saving still photos from the videos he made with his phone.

33. ALLEN's wife, S.S., advised agents she was aware of ALLEN watching and possessing child pornography for several years. The last image she saw was in May or June of 2021. S.S. advised ALLEN knows how to encrypt child pornography and he used multiple laptops to do so. She said ALLEN led her to believe he only accessed child pornography to save the minor victims and he encrypted the images/videos so the criminals could no longer gain access. She advised she has no knowledge or concerns of any inappropriate behavior with their eight children.

34. Children at the residence were forensically interviewed. Jane Doe described an incident where ALLEN forced her to bathe and recorded the incident. She stated that as part of the bath, he touched her everywhere except her genitals, including her breasts. When asked, ALLEN admitted to the same forcible bathing incident and to recording it as well. The forensic review of ALLEN's Samsung cellular phone revealed video stills of this incident, in which Jane Doe is naked.

35. Law enforcement conducted a probable cause arrest of ALLEN that morning and he was charged by criminal complaint on August 3, 2021, of one count of receipt of minors engaging in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(2), and one count of possession of images depicting minors engaged in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(4)(B). 2:21-mj-220, ECF No. 1 (signed by U.S. Magistrate Judge Douglas E. Miller). On August 9, 2021, ALLEN waived his preliminary hearing. A detention hearing was held and Judge Lawrence R. Leonard denied the government's motion for detention but granted the government's motion to stay his release order pending the government's appeal to the U.S. District Judge. ECF No. 12. That appeal remains pending.

36. On September 2, 2021, a grand jury returned a six-count indictment charging ALLEN with two counts of attempted production of child pornography, in violation 18 U.S.C. § 2251(a), three counts of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2), and one count of access with intent to view child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). 2:21-cr-107, ECF No. 24.

37. An HSI forensic examiner discovered that the child pornography and child exploitation images were located as thumbnails in either the device gallery cache, or an app cache. They were previously located on the device and apparently deleted, or were encrypted with a file encryption app such as KeepSafePhoto Vault (which is currently on this device with a paid account) and cannot be detected or decrypted by either Cellebrite or Magnet software. Keepsafe Photo Vault also utilizes a cloud backup, and has an account which is usually tied to an

email address. KeepSafe sends correspondence related to the account and to Keepsafe products and services to the e-mail address of record, including verification e-mails and billing e-mails.

38. "Keepsafe" is an application available for both Android and Apple devices that is offered and maintained by Keepsafe, Inc., a company based in San Francisco, California. The Keepsafe application permits account holders to conceal and secure personal photos and videos by locking them down on the device in "photo lockers" or "secret photo vaults" with password protection. In addition, Keepsafe, Inc. also provides account holders with photograph and video backup with cloud storage.

39. The following accounts were located on ALLEN's Samsung cellular phone: nathanallen88@gmail.com, policemannate88@gmail.com, natepitbull22@gmail.com, staceyandnatewedding2028@gmail.com, nallen@kingsmillpolice.org. On or about September 16th, 2021, SA Shields spoke to a representative of Keepsafe. They confirmed there was a Keepsafe account associated with the email nathanallen88@gmail.com, and it was a paid account. The representative confirmed the data associated with the account was preserved pending the receipt of a search warrant to disclose any additional information or data.

40. Android cellular phones, such as and including ALLEN's Samsung cellular phone, have factory installations of the Google suite of applications, including Gmail, Google Drive, Google Photos and others. The principal email account for ALLEN's Samsung cellular phone is the SUBJECT GOOGLE ACCOUNT, which account was therefore the one associated with the Google applications on the phone. The other Google email accounts identified in the preceding paragraphs were associated with other applications installed on the phone. The files stored on a cellular phone that has Google's cloud-based storage applications installed, such as Google Drive and Google Photos, can be automatically or manually synced with or uploaded to those storage applications. When asked, ALLEN did not deny that he had stored images in Google applications, but stated he was unsure whether any of the images were still saved on the Google cloud storage of the Google account associated with his phone.

BACKGROUND CONCERNING GOOGLE, EMAIL & CLOUD SERVICES

41. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A-2. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

42. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), chat logs, and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

43. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

44. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

45. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

46. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such

as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

SERVICE OF LEGAL PROCESS ON KEEPSAFE

47. Keepsafe, Inc. is located at 427 Bryant Street, San Francisco, California 94107.

48. I know that Keepsafe maintains records on their users, such as basic subscriber information within the meaning of 18 USC 2703(c)(2). Furthermore, I know Keepsafe keeps and maintains the stored content of their users' accounts, such as photographs, movies, documents, and music, all within the meaning of the Stored Communication Act.

49. According to Keepsafe's privacy policy, at https://www.getkeepsafe.com/privacy-policy/:

a. ***Account information***. We collect personal information when you create an account, such as your email address and password, as well as your phone number if you provide one to enable two-factor authentication or if you use our telephony service.

b. ***Account content***. If you have a Service account, you can use and store different types of data in the Service, such as photos and videos, files, messages and other content.

c. ***Transaction information.*** When you order paid versions of the Service we collect information necessary to complete the transaction, including your name, payment information and billing information.

d. ***Contact details***. We collect the contact details you share with us when you communicate with us, which may include your email address, phone number, postal address or social media handles.

e. ***Device and usage information.*** We use server logs, cookies and similar technologies to automatically collect information about your computer or device and how you interact with the Service. For example, we may record your application version, browser type, computer or mobile operating system, Internet Protocol (IP) address (a number that is automatically assigned to your computer or mobile device when you use the Internet, which may vary from session to session) and your unique device, application or advertising identifiers. In addition to information about your device, we collect information about how you interact with the Service, such as the page that referred you, your search terms, pages or areas of the Service you use or share, the time and duration of visits, features you used and links you clicked on.

f. ***Phone information.*** If you use the telephony or text messaging services available in some of our mobile applications, we may collect information related to your use of these services, such as the phone numbers you call and message and from which you receive calls and messages, the content of text messages, number of minutes used, number of text messages sent, and amount of data plan consumed.

CONCLUSION

50. As explained herein, information stored in connection with the SUBJECT ACCOUNTS may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with electronic accounts can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, electronic account communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the ESP can show how and when the account was accessed or used. For example, e-mail providers typically log the Internet Protocol (IP) addresses from which users access the e-mail account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the e-mail account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored in the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Lastly, stored electronic data may provide relevant insight into the electronic account owner's state of mind as it relates to the offense under investigation. For example, information in the e-mail account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

51. Based on the aforementioned factual information, I respectfully submit that probable cause exists to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(2) & (4)(B), which, in relevant part, prohibit the production, receipt, and knowing possession of or access with the intent to view one or more matters containing any visual depictions of are located within the SUBJECT ACCOUNTS.

52. Accordingly, I request that a warrant be issued authorizing me, law enforcement personnel, and forensic support personnel, to search the SUBJECT ACCOUNTS for, and seize, the items specified in Attachments B-1 and B-2.

53. Because the warrants will be served on Keepsafe and Google electronically or by mail, who will then compile the requested records at a time convenient to it, good cause exists to permit the execution of the requested warrants at any time in the day or night.

FURTHER AFFIANT SAYETH NOT.

John W. Shields, Special Agent
Homeland Security Investigations
Norfolk, VA

SUBSCRIBED and SWORN to before me on this 23rd day of September, 2021.

Honorable Lawrence R. Leonard
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information located within the Keepsafe account identified by and/or associated with the email account/address nathanallen88@gmail.com which is stored at premises owned, maintained, controlled, or operated by Keepsafe, Inc., a company headquartered at 427 Bryant Street, San Francisco, California 94107.

ATTACHMENT A-2

DESCRIPTION OF PROPERTY/LOCATION TO BE SEARCHED

This warrant applies to information located within the Google account identified by and/or associated with the email account/address nathanallen88@gmail.com which is stored and maintained at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be Disclosed by KeepSafe, Inc., (the "Provider")

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held, or maintained inside or outside of the United States, and including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the account listed in Attachment A-1 (the SUBJECT KEEPSAFE ACCOUNT), from the time of the account's creation to the present:

a. All records or other information stored by the subscriber or any other individual in or using the SUBJECT KEEPSAFE ACCOUNT, including, but not limited to, profile, address books, bookmarks, links to internet addresses, any and all audio/video files and photographic images (including deleted items), emails, instant messages, texts, contact and, and calendar datalists, and calendar data;

b. All transactional information of all activity of the SUBJECT KEEPSAFE ACCOUNT, including log files, messaging logs, records of session times and durations, dates and times of connecting, methods of connecting; email "invites" sent or received via Keepsafe, any contact lists, and Internet Protocol ("IP") or other identifying information related to any user who has accessed, downloaded and/or uploaded content from the SUBJECT KEEPSAFE ACCOUNT;

c. All records or other information regarding the identification of the SUBJECT KEEPSAFE ACCOUNT, to include full name, physical address, telephone numbers, e-mail addresses (including primary, alternate, rescue, and notification e-mail addresses, and verification information for each e-mail address), the date on which the SUBJECT KEEPSAFE ACCOUNT was created, the length of service, the IP address used to register the SUBJECT KEEPSAFE ACCOUNT, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

d. All records pertaining to communications between the Provider and any person regarding the SUBJECT KEEPSAFE ACCOUNT, including contacts with support services and records of actions taken.

e. All records and information regarding locations where the SUBJECT KEEPSAFE ACCOUNT was accessed, including all data stored in connection with location services; and

f. All records pertaining to the types of service used, including linked accounts based upon IP Addresses and session cookies.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

Notwithstanding 18 U.S.C. § 2252 or any similar statute or code, items to be delivered to the government pursuant to this search warrant may be sent on any digital media device or other electronic means to john.w.shields@ice.dhs.gov, or via mail to 200 Granby St., Suite 600, Norfolk, Va 23510.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(2) & (4)(B), including, for the SUBJECT KEEPSAFE ACCOUNT, information pertaining to the following matters:

a. The identity of the person(s) who created or used the SUBJECT KEEPSAFE ACCOUNT, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the SUBJECT KEEPSAFE ACCOUNT was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. All records pertaining to communications between the Provider and any person regarding the SUBJECT KEEPSAFE ACCOUNT.

e. Evidence indicating the subscriber or any other individual's state of mind as it relates to the crime under investigation;

f. Any person knowingly receiving, producing, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);

g. Any and all child pornography, meaning any visual depiction including, but not limited to, any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction appears to be of a minor engaging in sexually explicit conduct;

h. Child erotica materials, including, but not limited to images that may serve to gratify the sexual interest in children that may reveal a sexual preference, or that may evince a criminal intent to commit violations of 18 U.S.C. §§ 2251(a), (a)(2), and (a)(4)(B).

i. Evidence of the times the SUBJECT KEEPSAFE ACCOUNT was used;

j. Passwords and data security devices, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A-1 and other associated accounts; and

k. Device backups including camera roll and photo stream data to identify child pornography, victims or contraband.

ATTACHMENT B-2

Particular Things to be Seized

I. Information to Be Disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held, or maintained inside or outside of the United States, and including any messages, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the account listed in Attachment A-2 (the SUBJECT GOOGLE ACCOUNT), from the time of the account's creation to the present:

a. The contents of all e-mails and chat communications associated with the SUBJECT GOOGLE ACCOUNT, including stored or preserved copies of e-mails sent to and from the account, email attachments, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the types of service utilized, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, accounts' status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by at any time by any individual using the SUBJECT GOOGLE ACCOUNT, including chat logs, address books, contact and buddy lists, calendar data, pictures, videos and files, including in Google Drive, Google Docs, and Google Photos;

d. All records pertaining to communications between the Provider and any person regarding the SUBJECT GOOGLE ACCOUNT, including contacts with support services and records of actions taken; and

e. For all information required to be disclosed under this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

Notwithstanding 18 U.S.C. § 2252 or any similar statute or code, the Provider shall provide all responsive data by sending it via U.S. mail, courier, email or the Google LERS Portal to:

Special Agent John Shields
Homeland Security Investigations
200 Granby Street Suite 600
Norfolk, VA 23510
John.w.shields@ice.dhs.gov

II. Information to Be Seized by the Government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252(a)(2) & (4)(B), including, for the SUBJECT GOOGLE ACCOUNT, information pertaining to the following matters:

a. The identity of the person(s) who created or used the SUBJECT GOOGLE ACCOUNT, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the SUBJECT GOOGLE ACCOUNT was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

a. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

b. All records pertaining to communications between the Provider and any person regarding the SUBJECT GOOGLE ACCOUNT.

c. Evidence indicating the subscriber or any other individual's state of mind as it relates to the crime under investigation;

d. Any person knowingly receiving, producing, or possessing child pornography, as defined at 18 U.S.C. § 2256(8);

e. Any and all child pornography, meaning any visual depiction including, but not limited to, any photograph, film, video, picture, or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction appears to be of a minor engaging in sexually explicit conduct;

f. Child erotica materials, including, but not limited to images that may serve to gratify the sexual interest in children that may reveal a sexual preference, or that may evince a criminal intent to commit violations of 18 U.S.C. §§ 2251(a), (a)(2), and (a)(4)(B).

g. Evidence of the times the SUBJECT GOOGLE ACCOUNT was used;

h. Passwords and data security devices, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A-2 and other associated accounts; and

i. Device backups including camera roll and photo stream data to identify child pornography, victims or contraband.